(12) UK Patent Application (19) GB (11) 2 188 762 (13) A

(43) Application published 7 Oct 1987

(21) Application No 8608244

(22) Date of filing 4 Apr 1986

(51) INT CL⁴
G06K 5/00

(52) Domestic classification (Edition I):
G4H 13D 14A 14B 1A TG

(56) Documents cited
GB A 2060228
GB 1576463
GB 1559962
GB 1464703
GB 1458495
GB 1300848
GB 1294232
EP A2 0129139

(58) Field of search
G4H
Selected US specifications from IPC sub-classes G06K
G07F

(71) Applicants
Philip Hall Bertenshaw,
18 Lower Fold, Marple Bridge, Stockport, Cheshire
SK6 5DX.

John Jones,
82 Guywood Lane, Romiley, Stockport, Cheshire

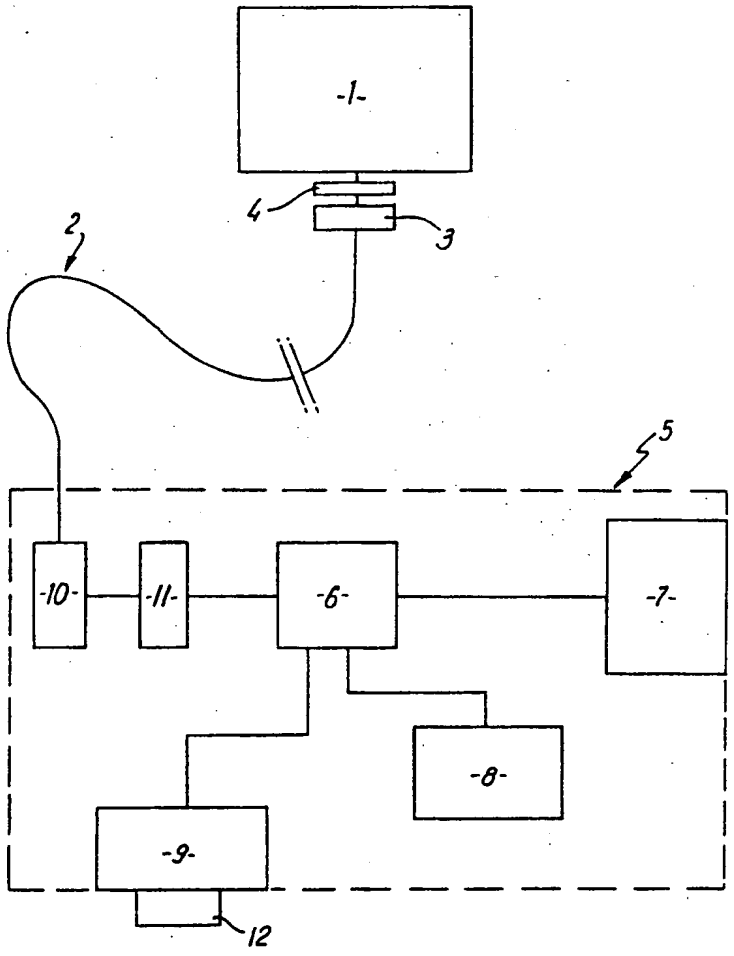
(72) Inventors
Philip Hall Bertenshaw
John Jones

(74) Agent and/or Address for Service
M'Caw & Co.,
41–51 Royal Exchange, Cross Street, Manchester
M2 7BD

(54) Secure data communication system

(57) A secure data communication system has one or more local terminals (5) connected, e.g. via modems (3,10), encryption/decryption units (4,11) and telephone network (2), to a remote data base (1). To transmit data, a security device in the local terminal (5) must be actuated first.

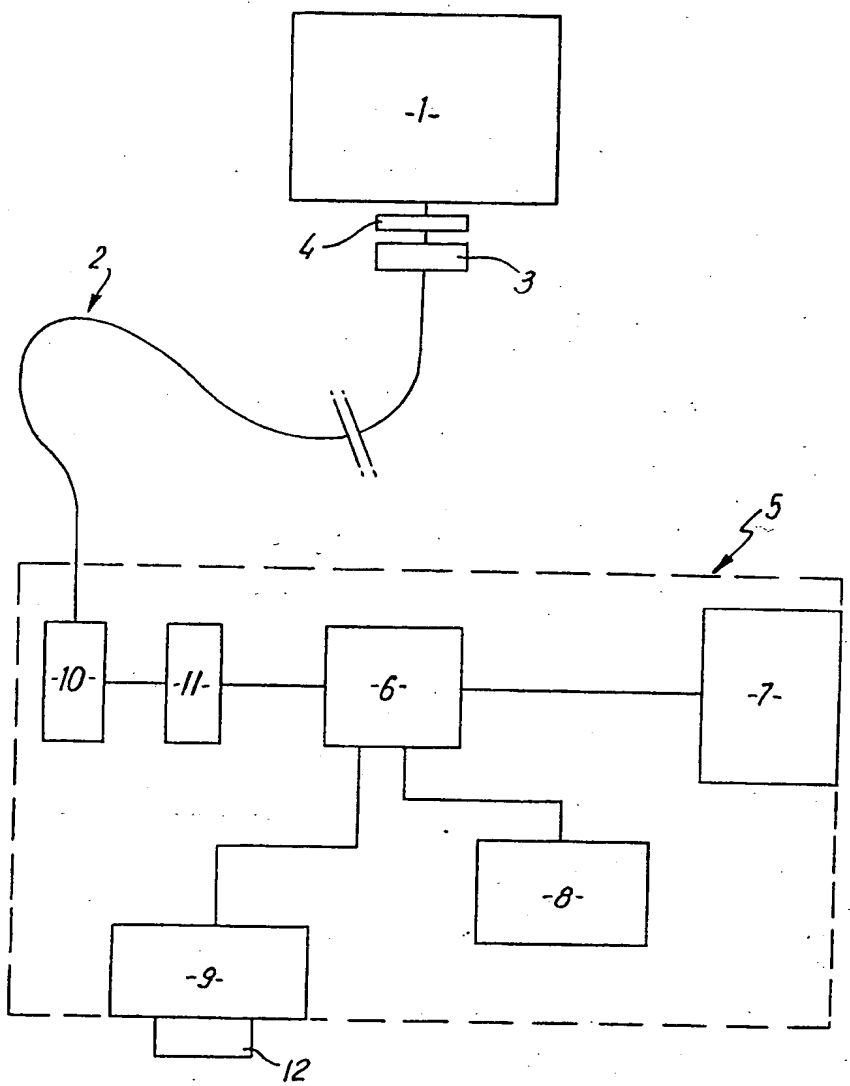
The security device comprises a code reader (9) into which a personal identification device (12) e.g. a card with a coded magnetic stripe, can be removably inserted. The card (12) may provide an identification code (compared with a code keyed in at 7) and also a key for the encryption/decryption. The reader (9) can change the code and key on the card (12) under control of the data base (1).



GB 2 188 762 A

The drawing(s) originally filed was/were informal and the print here reproduced is taken from a later filed formal copy.

The claims were filed later than the filing date within the period prescribed by Rule 25(1) of the Patents Rules 1982.



SPECIFICATION

Secur data communication syst m

This invention relates to a secure data communication system.

It is common practice to use the public telephone network as a data communication link between local terminals and a remote computerised data base. For security reasons it is known to encrypt the communicated data and this usually involves the incorporation of encryption/deencryption units in the local terminals with a fitted encryption key in each such unit. However, with this arrangement there is the problem of preventing unauthorised communication with the data base whilst permitting easy and convenient use of the terminals by authorised personnel. In particular, if there are different levels of security data using different encryption keys, it may be necessary to allocate different terminals to different authorised users.

An object of the present invention is to overcome or at least minimise the abovementioned problem.

According to the invention therefore there is provided a secure data communication system comprising at least one local terminal, at least one remote data handling device, interface devices arranged to connect such terminal and data handling device to a data communication link, and a security device at such terminal requiring actuation in order to permit data communication in a desired mode with such data handling device, characterised in that said security device has a code-reading device with which a coded portable personal identification device is removably locatable in interactive proximity for code reading purposes, said code-reading device being arranged to effect said actuation of said security device when a predetermined code is read from said identification device.

With this arrangement, it is possible to safeguard against unauthorised use of the terminal whilst at the same time permitting use by an authorised person in a particularly convenient manner. In this respect, the coding of the identification device may include a code word or number which is verified by the terminal, for example, by automatic cross-checking against a pre-programmed list of authorised codes, or by comparison with a code entered manually by the user via a keyboard.

The personal identification device may be in the form of a card although other structural forms are also possible. The mode of interaction with the code-reading device may be such that electrical contact or interconnection therebetween is not necessary. Thus, the code-reading device may be arranged to read a magnetic stripe on the identification device or it may be arranged to couple inductively with a circuit on the identification device as described in co-pending Application No. 8514219.

The system may be used with multiple differently coded personal identification devices. In this case, there may be multiple terminals and the arrangement may be such that any identification device can actuate any terminal or alternatively that each identification device can only actuate a respective one of the terminals. Advantageously, the terminals may be of standardised form and any required differences in operation thereof may be achieved by utilisation of different operational data derived from the codes of the respective identification devices. Thus, for example, the security device of the or each terminal may comprise an encryption and/or de-encryption device and the personal identification device which is used to actuate the respective terminal may be arranged to provide, in its coding, part or all of an encryption key necessary for the proper operation of the security device.

Most preferably, the code-reading device of the or each terminal is capable of writing to as well as reading from the personal identification device. In this way it is possible to achieve particularly good security in so far as the coding of the personal identification device can be changed or updated from time to time. For example, the identification device may carry, as part of its coding, a transaction number which is indexed each time the device is used and the system may be arranged to check the value of the transaction number against a stored transaction record in order to verify the identification device. Such writing and verification procedures may be effected locally and/or remotely. For example, the abovementioned indexing of the transaction number may be effected locally by the security device whereas the checking of the current value of the transaction number may be effected remotely at the data handling device. Other transactional information may be written to and read from the identification device such as date or duration of the last transaction etc. Moreover, part or all of the coding of the identification device, such as the abovementioned personal code word or code number and/or the abovementioned encryption key, can be changed at appropriate intervals, for example, after predetermined periods of time, after predetermined numbers of transactions or the like.

The invention will now be described further by way of example only and with reference to the accompanying drawing which is a diagrammatic view of one form of a communication system according to the invention.

As shown in the drawing, a secure communication system comprises a central computerised data base 1 which is connected to the public telephone network 2 via a modem 3 and an encryption/de-encryption unit 4.

Multiple identical terminals 5 are also con-

nected to the telephone network 2 at different locations remote from the data base 1. Only one terminal 5 is shown for the sake of convenience.

The terminal 5 comprises a microcomputer 6 with a connected keyboard 7 and vdu display 8. The microcomputer 6 is also connected to a reading device 9 and to the telephone network 2 via a modem 10 and an encryption/de-encryption unit 11.

Each person authorised to use the terminal 5 has a respective portable identification device which may be in the form of a "credit card" 12 with a magnetic stripe. The card 12 can be inserted into a slot in the reading device 9 so that coded information on the stripe can be read automatically by the reading device 9 and also so that information can be written by the reading device onto the stripe.

When a card 12 is inserted into the reading device 9 the information on the magnetic stripe is read and is verified in the first instance by the microcomputer 6. That is, the user enters a code word or number via the keyboard 7 and the microcomputer 6 checks to see if this is the same as a personal identification code which is on the card. The terminal 5 is then actuated to the extent that it is now possible to establish a communication link with the central data base 1, by dialling the communication number of the data base 1 in the usual way. Once communication has been established, data can be transmitted to and received from the data base 1 via the modem 10 and the encryption/deencryption unit 11. At this stage, for proper operation of the unit 4, an encryption key is required and this is read from the magnetic stripe on the card 12. This constitutes a further verification since intelligible data communication cannot take place if the correct key is not read from the card 12.

A further verification operation is carried out in that transactional information is read from the card and is checked by the central data base 1. For example, each time the card 12 is used, at the end of the transaction the reading device 9 under the local control of the microcomputer 6 reads a transaction number on the card and then overwrites this with a number which is one higher. The data base 1 stores a transaction record for each card and can check to see if the stored transaction number is equal to the number on the card. if desired other transactional information, such as the date of a transaction can be read, written, stored and checked.

The reading device 9 can also change the personal identification code and/or the encryption key on the card under the instructions of the data base 1. For example, the personal identification code may be changed periodically so that the card can only be used to actuate the terminal 5 by a person who is familiar with the current code to be entered via the keyboard. This periodic changing may be effected automatically at the end of or during a transaction when the card is first used following a predetermined change-over date. The encryption key may also be changed automatically likewise at the end of or during a transaction when the card is first used following a predetermined change-over date.

The reading device 9 may be arranged to eradicate the information stored on the card 12, under local or remote control, in the event that read information is not verified, for example, if three unsuccessful attempts are made to enter a correct personal identification code via the keyboard 7.

With the arrangement described above great security can be achieved in a particularly simple and convenient manner.

A user of the system can gain access to the data base 1 simply by inserting his identification card into the reading device 9 of any terminal 5 and entering his personal identification code via the keyboard 7.

Different personnel having different levels of security clearance can use the system even though the terminals 5 are of a common standardised form. This can be achieved conveniently because it is possible to provide different personal identification cards with different encryption keys so that the user can only gain access to data which is encrypted on the data base in a format corresponding to that person's encryption key.

It is of course to be understood that the invention is not intended to be restricted to the details of the above embodiment which are described by way of example only. Thus, although reference is made to telephone network it is to be understood that any other suitable form of communication link may be used between the data base 1 and the terminals 5.

CLAIMS

1. A secure data communication system comprising at least one local terminal, at least one remote data handling device, interface devices arranged to connect such terminal and data handling device to a data communication link and a security device at such terminal requiring actuation in order to permit data communication in a desired mode with such data handling device, characterised in that said security device has a code-reading device with which a coded portable personal identification device is removably locatable in interative proximity for code reading purposes, said code-reading device being arranged to effect said actuation of said security device when a predetermined code is read from said identification device.

2. A system according to claim 1 characterised in that the personal identification device is in the form of a card.

3. A system according to claim 1 or 2 char-

acterised in that there are multiple said terminals for use with multiple differently coded personal identification devices.

CLAIMS

4. A system according to claim 3 characterised in that the terminals are of standardised form and differences in operation thereof are achieved by utilisation of different operational data derived from the codes of the respective identification devices.

5. A system according to claim 4 characterised in that the security device of each terminal comprises an encryption and/or de-encryption device and the personal identification device which is used to actuate the respective terminal provides in its coding part or all of an encryption key necessary for the proper operation of the security device.

6. A system according to any one of claim 1 to 5 characterised in that the code-reading device of the or each terminal is capable of writing to as well as reading from the personal identification device.

7. A system according to claim 6 characterised in that the identification device carries as part of its coding a transaction number which is indexed each time the device is used and the system is arranged to check the value of the transaction number against a stored transaction record.

8. A system according to claim 7 characterised in that the indexing of the transaction number is effected locally by the security device whereas the checking of the currant value of the transaction number is effected remotely at the data handling device.

9. A system according to claim 1 substantially as hereinbefore described with reference to and as illustrated in the accompanying drawings.

Printed for Her Majesty's Stationery Office
by Burgess & Son (Abingdon) Ltd, Dd 8991685, 1987.
Published at The Patent Office, 25 Southampton Buildings,
London, WC2A 1AY, from which copies may be obtained.